



Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-17. (Canceled)

18. (Previously Presented) A data processing method comprising:

maintaining a database containing a table of data in row and column format, at least a portion of the data being encrypted;

maintaining, separate from the table of data, information for controlling access to a specified proper subset of data in the table; and

controlling access to the specified proper subset of data in the table according to the separately maintained information.

19. (Previously Presented) The method of claim 18, wherein controlling access comprises controlling access by a specified user or group of users.

20. (Previously Presented) The method of claim 18, wherein controlling access comprises controlling access by a specified program or group of programs.

21. (Previously Presented) The method of claim 18, wherein the separately maintained information comprises a separate table inaccessible to a user seeking access to the data.

22. (Previously Presented) The method of claim 18, wherein the separately maintained information comprises a separate table inaccessible to a program seeking access to the data.

- 23. (Previously Presented)** The method of claim 18, wherein controlling access to the specified proper subset of the data comprises using a tamper-resistant hardware module.
- 24. (Previously Presented)** The method of claim 23, wherein the tamper-resistant hardware module is used to perform a cryptographic operation on the data.
- 25. (Previously Presented)** The method of claim 23, wherein the tamper-resistant hardware module is used to store at least a portion of the separately maintained information.
- 26. (Previously Presented)** The method of claim 23, wherein the tamper-resistant hardware module comprises a hardware security module.
- 27. (Previously Presented)** The method of claim 23, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.
- 28. (Previously Presented)** The method of claim 18, wherein the specified proper subset of data comprises a specified column of data.
- 29. (Previously Presented)** The method of claim 18, wherein the information for controlling access comprises information used in encrypting or decrypting data in the proper subset of data.
- 30. (Previously Presented)** The method of claim 29, wherein the information used in encrypting or decrypting data comprises information identifying a way of encrypting or decrypting data in the proper subset of data.
- 31. (Previously Presented)** The method of claim 18, wherein the information for controlling access comprises information identifying an owner of the proper subset of data.
- 32. (Previously Presented)** The method of claim 18, wherein the information for controlling access comprises encrypted information.

33. (Previously Presented) The method of claim 18, further comprising:

receiving a request for access to a particular data element in the table, the particular data element containing encrypted data;

obtaining, from the separately maintained data, cryptographic information associated with a proper subset of data in the table, the proper subset containing the particular data element; and

decrypting the data in the particular data element using the cryptographic information.

34. (Previously Presented) The method of claim 33, wherein decrypting the data is done using a tamper-resistant hardware module.

35 (Previously Presented) The method of claim 34, wherein the tamper-resistant hardware module comprises a hardware security module.

36. (Previously Presented) The method of claim 34, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

37. (Previously Presented) The method of claim 18, further comprising

receiving a request for access to a particular data element in the table, the particular data element containing encrypted data; and

obtaining, from the separately maintained data, information associated with a proper subset of data in the table, the proper subset containing the particular data element; and

providing decrypted data from the particular data element when the information from the separately maintained data indicates that the request for access to the particular data element is an authorized request.

38. (Previously Presented) The method of claim 37, further comprising decrypting the data from the particular data element using a tamper-resistant hardware module.

39. (Previously Presented) The method of claim 38, wherein the tamper-resistant hardware module comprises a hardware security module.

40. (Previously Presented) The method of claim 38, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

41. (Currently Amended) A method comprising:

providing a database containing a table having at least two columns of data;

encrypting data in a first column using first cryptographic information;

encrypting data in a second column using second cryptographic information;

storing ~~[[the]]~~ first and second cryptographic information outside of the table;

controlling access to data in the first column using the first cryptographic information stored outside of the table; and

controlling access to data in the second column using the second cryptographic information stored outside of the table.

42. (Previously Presented) The method of claim 41, further comprising storing the first and second cryptographic information in a separate table inaccessible to a user seeking access to the data.

43. (Previously Presented) The method of claim 41, further comprising storing the first and second cryptographic information in a separate table inaccessible to a program seeking access to the data.

- 44. (Previously Presented)** The method of claim **41**, wherein the first and second cryptographic information are stored, in encrypted form, outside of the table.
- 45. (Previously Presented)** The method of claim **41**, wherein at least a portion of the data is encrypted using a tamper-resistant hardware module.
- 46. (Previously Presented)** The method of claim **45**, wherein the tamper-resistant hardware module comprises a hardware security module.
- 47. (Previously Presented)** The method of claim **45**, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.
- 48. (Previously Presented)** A database management system comprising:
- a database containing a table having at least two columns of data, at least one column of data being encrypted; and
- information stored outside of the table for controlling access to at least one column of data, the information including cryptographic information associated with the encrypted column of data.
- 49. (Previously Presented)** The system of claim **48**, wherein the information is stored in a separate table inaccessible to a user seeking access to the data.
- 50. (Previously Presented)** The system of claim **48**, wherein the information is stored in a separate table inaccessible to a program seeking access to the data.
- 51. (Previously Presented)** The system of claim **48**, wherein the information is stored in encrypted form.

52. (Previously Presented) The system of claim 48, further comprising a tamper-resistant hardware module for performing cryptographic operations on the encrypted column of data.

53. (Previously Presented) The system of claim 52, wherein the tamper-resistant hardware module comprises a hardware security module.

54. (Previously Presented) The system of claim 52, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

55. (Cancelled)

56. (Previously Presented) A data processing method comprising:

maintaining a first set of data as a collection of records having fields, at least a portion of the data being encrypted;

maintaining, separate from the first set of data, information for controlling access to a specified proper subset of the first data; and

controlling access to the specified proper subset of the first set of data according to the separately maintained information.

57. (Previously Presented) The method of claim 56, wherein controlling access comprises controlling access by a specified user or group of users.

58. (Previously Presented) The method of claim 56, wherein controlling access comprises controlling access by a specified program or group of programs.

59. (Previously Presented) The method of claim 56, wherein the separately maintained information comprises information that is inaccessible to a user seeking access to the data.

- 60. (Previously Presented)** The method of claim **56**, wherein the separately maintained information comprises information that is inaccessible to a program seeking access to the data.
- 61. (Previously Presented)** The method of claim **56**, wherein controlling access to the specified proper subset of the data comprising using a tamper-resistant hardware module.
- 62. (Previously Presented)** The method of claim **61**, wherein the tamper-resistant hardware module is used to perform a cryptographic operation on the data.
- 63. (Previously Presented)** The method of claim **61**, wherein the tamper-resistant hardware module is used to store at least a portion of the separately maintained information.
- 64. (Previously Presented)** The method of claim **61**, wherein the tamper-resistant hardware module comprises a hardware security module.
- 65. (Previously Presented)** The method of claims **61**, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.
- 66. (Previously Presented)** The method of claim **56**, wherein the specified proper subset of data comprises a specified field of data.
- 67. (Previously Presented)** The method of claim **56**, wherein the information for controlling access comprises information used in encrypting or decrypting data in the proper subset of data.
- 68. (Previously Presented)** The method of claim **56**, wherein the information for controlling access comprises information identifying an owner of the proper subset of data.
- 69. (Previously Presented)** The method of claim **56**, wherein the information for controlling access comprises encrypted information.

70. (Previously Presented) The method of claim **56**, further comprising:

receiving a request for access to a particular data element in the first set of data, the particular data element containing encrypted data;

obtaining, from the separately maintained data, cryptographic information associated with a proper subset of the first set of data, the proper subset containing the particular data element; and

decrypting the data in the particular data element using the cryptographic information.

71. (Previously Presented) The method of claim **70**, wherein decrypting the data is done using a tamper-resistant hardware module.

72. (Previously Presented) The method of claim **71**, wherein the tamper-resistant hardware module comprises a hardware security module.

73. (Previously Presented) The method of claim **71**, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

74. (Previously Presented) The method of claim **70**, wherein the proper subset comprises data in one or more specified fields.

75. (Previously Presented) The method of claim **56**, further comprising

receiving a request for access to a particular data element in the first set of data, the particular data element containing encrypted data; and

obtaining, from the separately maintained data, information associated with a proper subset of data in the first set of data, the proper subset containing the particular data element; and

providing decrypted data from the particular data element when the information from the separately maintained data indicates that the request for access to the particular data element is an authorized request.

76. (Previously Presented) The method of claim **75**, further comprising decrypting the data from the particular data element using a tamper-resistant hardware module.

77. (Previously Presented) The method of claim **76**, wherein the tamper-resistant hardware module comprises a hardware security module.

78. (Previously Presented) The method of claim **76**, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.

79. (Previously Presented) A method comprising:

providing a database containing at least two columns of data;

encrypting data in a first column using first cryptographic information;

encrypting data in a second column using second cryptographic information;

storing the first and second cryptographic information apart from the two columns of data;

controlling access to data in the first column using the first cryptographic information;
and

controlling access to data in the second column using the second cryptographic information.

- 80. (Previously Presented)** The method of claim 79, further comprising storing the first and second cryptographic information in a location that is inaccessible to a user seeking access to the data.
- 81. (Previously Presented)** The method of claim 79, further comprising storing the first and second cryptographic information in a location that is inaccessible to a program seeking access to the data.
- 82. (Previously Presented)** The method of claim 79, wherein the first and second cryptographic information are stored, in encrypted form, outside of the first and second column.
- 83. (Previously Presented)** The method of claim 79, wherein at least a portion of the data is encrypted using a tamper-resistant hardware module.
- 84. (Previously Presented)** The method of claim 83, wherein the tamper-resistant hardware module comprises a hardware security module.
- 85. (Previously Presented)** The method of claim 83, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.
- 86. (Previously Presented)** A database management system comprising:
- a database containing at least two columns of data, a first column of data being encrypted; and
 - information stored outside of the first column of data for controlling access to the first column of data, the information including cryptographic information associated with the first column of data.
- 87. (Previously Presented)** The system of claim 86, where in the information is stored in a location that is inaccessible to a user seeking access to the first column of data.

- 88. (Previously Presented)** The system of claim **86**, where in the information is stored in a location that is inaccessible to a program seeking access to the first column of data.
- 89. (Previously Presented)** The system of claim **86**, wherein the information is stored in encrypted form.
- 90. (Previously Presented)** The system of claim **86**, further comprising a tamper-resistant hardware module for performing cryptographic operations on the first column of data.
- 91. (Previously Presented)** The system of claim **90**, wherein the tamper-resistant hardware module comprises a hardware security module.
- 92. (Previously Presented)** The system of claim **90**, wherein the tamper-resistant hardware module is selected from the group consisting of a hardware security appliance and a cryptographic card.
- 93. (Cancelled)**
- 94. (New)** The method of claim **18**, further comprising revealing an unauthorized access to the data.
- 95. (New)** The method of claim **41**, wherein controlling access to data in the first column comprises revealing unauthorized access to the data.
- 96. (New)** The method of claim **56**, wherein controlling access comprising revealing unauthorized access to the first set of data.
- 97. (New)** The method of claim **79**, wherein controlling access to data in the first columns comprises revealing unauthorized access to the data.
- 98. (New)** The system of claim **48**, wherein the information stored outside of the table comprises information for revealing unauthorized access to the database.

Applicant : Ulf Dahl
Serial No. : 09/840,188
Filed : April 24, 2001
Page : 13 of 20

Attorney's Docket No.: 17299-008002

99. (New) The system of claim **86**, wherein the information stored outside of the table comprises information for revealing unauthorized access to the database.